山東藝術學院
SHANDONG UNIVERSITY OF ARTS

山东省教育系统网络安全工作经验交流稿

山东艺术学院信息中心主任 李政

2016年12月

山东艺术学院信息中心


山東藝術學院
信息中心
Information Center of SDCA
学院主页
部门首页
部门概况
领导机构
管理规章
联系方式
办事流程
下载专区
数据中心IDC
专业的机房环境，7*24小时贴心服务
网站托管
服务器托管
网络维护
校园卡服务
科室链接
网络建设科
Network construction department
信息资源建设科
The construction of Information Resources Department
部门动态
山东服装职业学院一行来信息中心考察交流
内蒙古艺术学院一行到信息中心考察交流
信息中心召开消防安全"五个治理"、网络安全等部署
党建工作
学习材料：党委会的工作方法
NEW
更多内容

做好网络信息安全工作

引言

- 校园网网络信息安全是一个系统工程，涉及到方方面面。当前各种各样的网络安全问题层出不穷，高校日益成为网络攻击的重灾区，各种各样的安全问题威胁着校园网的正常运行，给学校的教学、科研、管理、对外交流等带来重大影响，加强校园网络信息安全已经成为当前各高校信息化建设中不可忽视的一个重要问题。
- 按照国家和山东省教育厅的有关文件精神，我校对网络安全工作高度重视，为确保网络安全，采取了一系列举措，对照刚刚颁布的《中华人民共和国网络安全法》，将我校在网络安全工作方面的具体做法，向各位领导和专家汇报。

一、领导重视，提高对信息安全的要求

- 我校成立了信息化工作小组，高度重视信息安全工作。
- 首先，信息化工作小组定期组织学校信息化骨干认真学习领会国家的各类网络信息安全相关的文件。
- 其次，在实际工作中我中心领导提高了对信息安全的标准，坚持用信息系统等级保护条例的要求来衡量各信息系统，并于今年五月份专门请省信总的维平保测评公司对我校的网络信息建设进行了一次系统测评，并给出了测评报告。
- 根据测评报告，我中心对比不足制定了信息安全建设整改方案，在今年六月份进行了一次信息安全建设全面整改活动，从物理安全、网络安全、主机安全、应用安全、数据安全五大方面进行整改，整改中领导要求可以做到的项目必须要做好，没有条件完成的项目也要标识清楚原因。我校目前正在进行的智慧校园建设项目在结项时也会遵循这五大方面进行严格审核。

二、加大规章制度的编制和工作执行力度

- 我中心重视制度建设，多次组织各职能科室建立系统的管理规章和安全管理制度，建有一系列的网络信息安全管理规章制度，通过制度的制定与实施，中心要求大家在工作中要严格按规章制度办事。切实让相关人员担负起对网络信息安全的监督、管理工作责任。

二、加大规章制度的编制和工作执行力度

- **网络安全方面**：网络安全管理制度包括两类或者叫两维，一类是综合的网络信息安全管理规章制度，像《网络设备密码管理制度》、《校园网综合布线检修制度》、《中心机房管理制度》等属于第一维度的管理制度，另一类是针对某个具体设备的使用和管理的规章制度。尤其是第二类的管理制度，制度的条目必须清晰，可执行性必须明确。设备使用的权限和责任必须落实到具体个人，相关使用过程必须要有可回溯的材料。《新一代防火墙管理制度》、《认证账号管理制度》、《VPN使用管理制度》、《邮箱使用管理制度》等，这些都是属于具体设备使用的管理制度，属于第二维度。

二、加大规章制度的编制和工作执行力度

- 信息安全方面：我校的信息安全管理制度是在具体工作实践过程中逐渐建立、修订、完善起来的。在2002年我校开始进行信息化建设，学校各职能处室开始建立自己的网站，为规范网站信息发布，我校制定《网上信息发布授权责任书》对普通人员的信息发布行为进行严格规范，并对日常密码、信息备份等工作给出指导性意见。在今年的智慧校园一期工程中引入了站群管理系统，我们及时制定《站群系统子站建设管理办法（草案）》来规范站群的使用。13年开始提供虚拟服务器免费借用服务，为学校各处室提供免费的虚拟服务器使用，所有申请者均填写《虚拟服务器申请表》，以便进行虚拟服务器资源的管理。近年来，我们学校很多职能处室都购置了相关业务信息系统，我中心在多方面考察后根据实际情况制定《托管服务器管理办法》，其服务器均托管在我中心，所有托管服务器均填写《服务器托管登记表》，每个系统独立建档，按照“谁使用谁负责”的原则，做到责任到人。

三、坚持原则，规范信息系统工作程序

- 我校多年来一直坚持集中管理的原则，规范各类信息系统发布的工作程序。新的信息系统入网时必须要登记；新的网站入网时也必须要领导审核同意在我中心备案后才能发布；新的校园网用户入网账号口令必须要登记，实行实名制上网；所有信息系统和账号口令使用时要责任到人。严格限制内部人员私自在公网上发布信息系统。严格限制内部人员私自接入外网。具体的信息发布要求各职能部门有一套完整的内容审核程序，防止信息泄密。我中心对登记的信息系统进行建档管理，定期查看状态，并使用趋势科技杀毒服务软件进行病毒监控，根据登记的服务和端口在WAF和防火墙等安全设备上做具体安全设置，在校外一律采用VPN方式进行管理。

四、加强队伍建设，强化安全意识

- 由于校内多个职能部门的信息系统使用人往往不是计算机相关专业的,计算机安全和服务器使用维护的安全意识相对比较淡薄,这就要求我们对信息源接入的骨干人员进行安全教育和培训，一是使之自觉遵守和维护《计算机信息网络国际互联安全保护管理办法》，杜绝发布违犯《计算机信息网络国际互联网安全保护管理办法》的信息内容;二是使之具备安全使用信息系统和对重要数据进行备份的能力。由于职能部门的业务比较繁忙，有时会忘记备份数据、定期更改口令、给系统打补丁、修复漏洞，我们的做法是QQ群消息通知和定期电话提醒，对于操作有困难的部门，约定时间上门服务，和使用人员一起打补丁、修复漏洞、备份数据，这样每一次都是一次现场培训，一个学期下来，他们基本上就能掌握这些步骤和操作流程。在有重大漏洞或有安全事件节点发布时，我们会特别提醒相关人员做好检查。

五、重视技术，增加资金投入建设

- 我校前后多次引入建行、联通等社会资金进行校园信息化建设，按照国家网络安全要求购置了相应网络安全设备及信息化设备。
- 为了确保网络信息安全，2014年我们购置或升级了包括防火墙、WAF、VPN等网络安全设备。设置三级防火墙体系，校园网出口防火墙作为第一级，在服务器前端部署第二级防火墙，服务器本身的软件防火墙作为第三级防火墙。在防火墙的使用过程中做到以下两点，一是配置最严格的策略，默认禁止所有，只允许需要的数据通过防火墙，二是定期及时检查防火墙上配置的策略，不再使用的策略及时删除。为弥补防火墙的不足，严格限制内部人员私自接入外网。学校的网站由专用的WAF设备防护，部分网站需要远程登录的情况，我们通过VPN技术来实现，对VPN账号的开设和管理仅限于有权限的相关人员。

五、重视技术，增加资金投入建设

- 为了确保网站信息安全，今年校方统一采购了网站群系统，并通过技术手段将所有部门、学院网站逐个迁移到网站群系统中来，实现了web程序代码的统一安全管理。在网站群系统中部署网页防篡改功能，如果发现网页有修改信息，可实时修复并报警。网站群整站备份对网站群中的所有文件、数据打包备份，如发生信息安全事件，则只需将网站群备份包上传至系统并恢复，以确保系统的适应性和稳定性。

六、人防技防结合，构建立体安全防御体系

- 技术设备再好，也离不开工作人员的日常检查和精心维护。信息安全工作必须从一点一滴做起，做好日常管理工作，发现问题后及时处理，才能最短时间内化解危机，把危险降到最低。
- 针对主机安全、网站安全、信息系统安全， 我院技术与管理两手一起抓，构建安全防御体系。

六、人防技防结合，构建立体安全防御体系

- 对于主机安全，我中心管理人员做到最基本的以下几点：1、定期更换高强度的系统管理员密码。2、升级系统。定时打各种补丁来保护系统安全，规避可能系统错误。3、软件维护。定期升级软件，修复BUG，关掉不必要的随机启动程序和服务。4、数据维护。数据备份是一个经常性的工作要定时本地、异地备份。5、安全维护。系统往往会存在还没有发现的安全漏洞，通过检查数据库、系统的运行日志，甄别攻击行为，并进行防范。6、及时的更新病毒库，查杀病毒。7、定时查看系统各个盘符的磁盘权限，是否为设定的安全权限。8、不随意使用不安全外部设备连接服务器或不安全电脑远程连接服务器，以免透过远程连接到服务器，使服务器成为被攻击的目标。9、经常检查系统是否多出超级管理员，检查是否有帐号被克隆。10、不要用服务器做和工作不相干的其他事情 。

六、人防技防结合，构建立体安全防御体系

- 对于网站安全，我中心在今年采购网站群系统之前，一直托管着全校各职能单位的所有官方网站。网站web程序代码多样化，非常不易管理。在这种情况下，我校之所以做到了零篡改的记录，除了对网站主机做到以上主机安全的几点之外，还有其他几点需要重点设置：1、定期检查关键目录文件夹如上传文件夹和数据库文件夹的状态及内容；2、把不需要随时改动的文件设为只读；3、把关键目录在IIS中的代码执行权限去掉，这样及时被攻击上传了后门木马，也无法被执行；4、修改数据库在IIS中的指向，必须数据库被下载，管理员密码被破解；5、隐藏伪装登录管理页面，避免使用通常默认的名字；6、定期按日期检索新增文件记录，发现问题及时处理；7、做好网站备份和数据库备份；8、督促网站管理员定期修改并保管好密码等等。

六、人防技防结合，构建立体安全防御体系

- 对于信息系统安全，我中心按照具体信息应用对其进行分级别管理。保密级别最高的信息系统必须只能不联网，只保持单机使用，如财务系统、组织部系统等；保密级别较高的信息系统必须只能校内访问，如档案系统、资产系统；保密级别一般的信息系统则设定校内校外访问，只在防火墙上打开必要的端口，并把易受攻击的普通默认端口数改成其他数，并加强维护和管理，管理服务器的时候要求必须以安全加密方式连接,校外使用VPN连接。

结语

- 以上只是我们的一些做法，敬请各位领导和同仁指正。
- 再次感谢厅信息中心领导举办此次培训班，感谢给我提供机会同大家交流工作心得！
- 祝我们的信息化明天更加美好！
- 谢谢大家！